DE1484

In the Claims:

Claim 1. (Amended) A method for identification, comprising the steps of:

(a) generating system parameters G_1, G_2, P and $\hat{e}$ and storing the system parameters in a memory by a system administrator, wherein G_1 and G_2 are cyclic groups of order m, P is a generator on the cyclic group G_1, $\hat{e}$ is a bilinear map defined as

$$\hat{e}: G_1 \times G_1 \mapsto G_2;$$

(b) generating a private key $<a, b, c>$ and a public key v and storing the public key v in the memory by a prover or the system administrator, wherein a, b and c are randomly chosen in Z_m^* where Z_m^* is a multiplicative group of order m;

(c) generating random numbers $r_1, r_2, r_3 \in Z_m^*$ for obtaining an evidence (x, Q) and sending the evidence (x, Q) to a verifier by the prover;

(d) receiving the evidence (x, Q), selecting a randomly selected number ~~$\omega \boxminus Z_m^*$~~ $\underline{\omega \in Z_m^*}$ to obtain a query R, storing the evidence (x, Q) and the randomly selected number ω in the memory and sending the query R to the prover by the verifier;

(e) receiving the query R, computing a temporary value S to obtain a response Y and sending the response Y to the verifier by the prover; and

(f) determining a legitimacy of the prover by employing the system parameters G_1, G_2, P and $\hat{e}$, the public key v, the evidence (x, Q) and the randomly selected number ω by the verifier.

Claim 2. (Original) The method of claim 1, wherein, in the step (b), the public key v is obtained by $v=\hat{e}(P, P)^{abc}$.

Claim 3. (Original) The method of claim 2, wherein, in the step (c), the evidence (x, Q) includes a first evidence value $x=\hat{e}(P, P)^{r_1 r_2 r_3}$ and a second evidence value $Q=r_1 r_2 r_3 P$.

Claim 4. (Original) The method of claim 3, wherein, in the step (d), the query R is obtained by $R=\omega P$.

Claim 5. (Original) The method of claim 4, wherein, in the step (e), the temporary value S is obtained by $S=r_1 r_2 r_3 R$ and the response Y is obtained by $Y=abcP+(a+b+c)S$.

Claim 6. (Original) The method of claim 5, wherein the verifier determines the legitimacy of the prover by verifying

$$\begin{aligned}
\hat{e}(Y,P) &= \hat{e}(abcP+(a+b+c)S,P) \\
&= \hat{e}(abcP+(a+b+c)r_1r_2r_3R,P) \\
&= \hat{e}(abcP+(a+b+c)r_1r_2r_3\omega P,P) \\
&= \hat{e}((abc+(a+b+c)r_1r_2r_3\omega)P,P) \\
&= \hat{e}(P,P)^{abc+(a+b+c)r_1r_2r_3\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(P,P)^{(a+b+c)r_1r_2r_3\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(P,r_1r_2r_3P)^{(a+b+c)\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(P,Q)^{(a+b+c)\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}((a+b+c),PQ)^{\omega} \\
&= \hat{e}(P,P)^{abc} \cdot \hat{e}(aP+bP+cP,Q)^{\omega} \\
&= v \cdot \hat{e}(aP+bP+cP,Q)^{\omega}
\end{aligned}$$

Claim 7. (Amended) A method for identification, comprising the steps of:

(a) generating system parameters G_1, G_2, P and $\hat{e}$ and storing the system parameters in a memory by a system administrator, wherein G_1 and G_2 are cyclic groups of order m, P is a generator on the cyclic group G_1, $\hat{e}$ is a bilinear map defined as

$$\hat{e}: G_1 \times G_1 \mapsto G_2;$$

(b) generating a private key $<a_1, a_2, \ldots a_n>$ and a public key v and storing the public key v in the memory by a prover or the system administrator, wherein $a_1, a_2, \ldots a_n$ are randomly chosen in Z_m^* where Z_m^* is a multiplicative group of order m;

(c) generating random numbers $r_1, r_2, \ldots r_n \in Z_m^*$ for obtaining an evidence (x, Q) and sending the evidence (x, Q) to a verifier by the prover;

(d) receiving the evidence (x, Q), selecting a randomly selected number ~~$\omega \in Z_m^*$~~ $\underline{\omega \in Z_m^*}$ to obtain a query R, storing the evidence (x, Q) and the randomly selected number ω in the memory and sending the query R to the prover by the verifier;

(e) receiving the query R, computing a temporary value S to obtain a response Y and sending the response Y to the verifier by the prover; and

(f) determining a legitimacy of the prover by employing the system parameters G_1, G_2, P and $\hat{e}$, the public key v, the evidence (x, Q) and the randomly selected number ω by the verifier.

Claim 8. (Original) The method of claim 7, wherein, in the step (b), the public key v is obtained by $v = \hat{e}(P, P)^{a_1 a_2 \cdots a_n}$.

Claim 9. (Original) The method of claim 8, wherein, in the step (c), the evidence (x, Q) includes a first evidence value $v = \hat{e}(P, P)^{r_1 r_2 \cdots r_n}$ and a second evidence value $Q = r_1 r_2 \ldots r_n P$.

Claim 10. (Original) The method of claim 9, wherein, in the step (d), the query R is obtained by $R=_{\omega}P$.

Claim 11. (Original) The method of claim 10, wherein, in the step (e), the temporary value S is obtained by $S = r_1r_2...r_nR$ and the response Y is obtained by $Y = a_1a_2...a_nP + (a_1+a_2+...+a_n)S$

Claim 12. (Original) The method of claim 11, wherein the verifier determines the legitimacy of the prover by verifying

$$\hat{e}(Y, P)= \hat{e}(a_1a_2...a_nP + (a_1+a_2+...+a_n)S, P)$$

$$= \hat{e}(a_1a_2...a_nP + (a_1+a_2+...+a_n)r_1r_2...r_nR, P)$$

$$= \hat{e}(a_1a_2...a_nP + (a_1+a_2+...+a_n)r_1r_2...r_n\omega P, P)$$

$$= \hat{e}((a_1a_2...a_n + (a_1+a_2+...+a_n)r_1r_2...r_n\omega)P, P)$$

$$= \hat{e}(P, P)^{a_1a_2...a_n+(a_1+a_1+...+a_n)r_1r_2...r_n\omega}$$

$$= \hat{e}(P, P)^{a_1a_2...a_n} \cdot \hat{e}(P, P)^{(a_1+a_1+...+a_n)r_1r_2...r_n\omega}$$

$$= \hat{e}(P, P)^{a_1a_2...a_n} \cdot \hat{e}(P, r_1r_2...r_nP)^{(a_1+a_1+...+a_n)\omega}$$

$$= \hat{e}(P, P)^{a_1a_2...a_n} \cdot \hat{e}(P, Q)^{(a_1+a_1+...+a_n)\omega}$$

$$= \hat{e}(P, P)^{a_1a_2...a_n} \cdot \hat{e}((a_1+a_2+...+a_n), PQ)^{\omega}$$

$$= \hat{e}(P, P)^{a_1a_2...a_n} \cdot \hat{e}(a_1P+a_2P+...+a_nP, Q)^{\omega}$$

$$= v \cdot \hat{e}(a_1P+a_2P+...+a_nP, Q)^{\omega}.$$